VOLUME 2, ISSUE 2

AUGUST 2009

InsighT to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter

Gmail Vulnerability Shows Importance of Strong Passwords

What's the big deal?

A recently discovered back door (reported by Vicente Aguilera Diaz on the Full Disclosure security list) into Gmail is another reminder that we need to use strong passwords. The vulnerability allows criminals to repeatedly guess passwords without being locked out. Gmail is – by no means – the only application vulnerable, but it is widely used and often considered to be more secure than other options.

Aguilera has reported that if someone has a Gmail account, they are able to guess another Gmail user's password up to 100 times in two hours; up to 1,200 guesses per day per account. Many hackers have over a hundred Gmail accounts, so they could create an automated tool which will guess against that many other accounts. If those accounts have weak passwords, this method will eventually enable a

In this Issue:

Strong Passwords (from page 1)

hacker into that account.

Complex but memorable

The only good way to defend yourself on line when accessing any account, e-mail, bank, file store, network, etc., is to have a strong password that is memorable. Many experts agree that the easiest way to do this is to use passphrases or signin phrases for your password. While you will have no problem remembering them, others will find it virtually impossible to guess.

Though Gmail does require a password of at least 8 characters, which is essential for basic security, it doesn't enforce complexity in the password. A user could have choose extremely weak passwords, such as 12345678, or samjones, or even zzzzzzzz.

Fido1212 or P@ssw0rd

Many people still choose to use pet or children's names, birthdays, or a common dictionary word. This means that their Gmail (or other accounts) could be guessed in less than 10,000 tries. Sometimes they even use the same password for every website. Plus, some people have a document on their computer which holds their passwords (and it isn't encrypted, or password protected itself) making their passwords vulnerable to a myriad of viruses, spywares and Trojans as well as hackers.

The 3 basic requirements for a strong password are length, unpredictability, and complexity (using different types of characters). Each extra character dramatically increases the potential combinations that a hacker would have to try to crack your password. See the table on the last page to see how dramatic this effect is.

Since the longer passwords work, you can choose passphrases, rather than passwords. There are a couple ways to do this, but always be sure to use Upper case, Lower Case, Numbers and Special Characters. Choose a song lyric, quote, poem, or bible phrase that you will remember, such as "How do I love thee, let me count the ways."

Using the first method, you would turn this into a relatively short password by using he first letter of each word and modifying others: "LU?Im456tw", shortening the first part of the line to "love you?" still gets the point across, then use "U" for you or thee, and "456" for count.

The second method yields a longer passphrase, but it's easier to type and equally impossible for an automated cracking tool to break. You could use just the second part of the line: "Let me 789 the ways!" Remember that spaces are special characters in Windows systems and many others. Try it; you'll see that your passphrase is much easier to type. Enjoy your new security!

Keep your strong passwords safe – Do's and Don'ts

(from and article in Windows Secrets by Becky Waring)

How do you protect your password?

First, create strong password, based on guidance from the main article in this newsletter. Now, follow these tips for using and protecting your password.

DO use a password manager such as

KeePass; http://sourceforge.net/projects/keepass/
Siber Systems Roboform http://www.roboform.com/

Citi-Software Access Manager http://download.lockergnome.com/Citi-Software-Ltd-publisher-87822.html

There are others but be careful that you're getting it from a legitimate source

DO change passwords frequently. I change mine every six months or whenever I sign in to a site I haven't visited in long time. Don't reuse old passwords. Password managers can assign expiration dates to your passwords and remind you when the passwords are about to expire.

DO keep your passwords secret. Putting them into a file on your computer, e-mailing them to others, or writing them on a piece of paper in your desk is tantamount to giving them away. If you must allow someone else access to an account, create a temporary password just for them and then change it back immediately afterward.

No matter how much you may trust your friends or colleagues, you can't trust their computers. If they need ongoing access, consider creating a separate account with limited privileges for them to use.

DON'T use passwords comprised of dictionary words, birthdays, family and pet names, addresses, or any other personal information. Don't use repeat characters such as **111** or sequences like **abc, qwerty,** or **123** in any part of your password.

DON'T use the same password for different sites. Otherwise, someone who culls your Facebook or Twitter password in a phishing exploit could, for example, access your bank account.

DON'T allow your computer to automatically sign in on boot-up and thus use any automatic e-mail, chat, or browser login. Avoid using the same Windows login password on two different computers.

DON'T use the "remember me" or automatic login option available on many Web sites. Keep logins under the control of your password manager instead.

DON'T enter passwords on a computer you don't control — such as a friend's computer — because you don't know what spyware or keyloggers might be on that machine.

DON'T access password-protected accounts over open Wi-Fi networks — or any other network you don't trust — unless the site is secured via **https.** Use a VPN if you travel a lot.

DON'T enter a password or even your account name in any Web page you access via an e-mail link. These are most likely phishing scams. Instead, enter the normal URL for that site directly into your browser, and proceed to the page in question from there.

Office of the CIO, Cyber Security Newsletter

650 W State St
Boise ID 83720

Phone: 208-332-1851
Email: terry.pobst-martin@cio.idaho.gov

CHECK OUT THESE LINKS

Links Websites about Rogue AV:

Good websites to surf:

http://www.sans.org/

http://www.cert.org/

http://www.msisac.org/

http://csrc.nist.gov/

http://www.issa.org/

http://www.infragard.net/

http://www.ic3.gov/

http://www.securityfocus.com/

http://www.snopes.com/

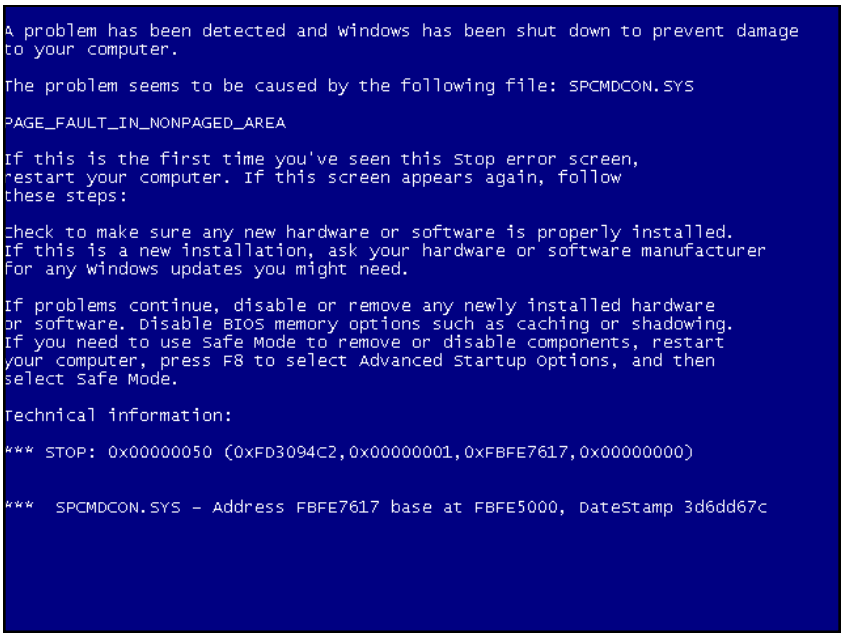
http://www.nationalterroralert.com/

Taking care of your own computer security relieves your worries so you can use your computer and enjoy it even more.

Quick Security Highlights

This month, Microsoft released nine security bulletins. Five of those are rated Critical and four have an aggregate severity rating of Important. Of the nine updates, eight affect Windows and the last one affects Office Web Components (OWC). Microsoft expects that there could be active hacking attempts to compromise your computers if you don't patch them right away. One of the quickest ways to ensure your computer is updated is to open Internet Explorer, click on "**Tools**" and choose "**Windows Update**". Then, when you're at the Microsoft update website, choose "**Express**" to get your high priority updates.

Malicious Software: A new "Scareware" package mimics the Windows "Blue Screen of Death." Miscreants have developed a scareware package that mimics Windows' infamous Blue Screen of Death. Potential victims see this bluse screen which normally shows the computer has crashed system. However, this screen also shows a text warning that they need to buy "security software" to clean up their systems. But the SystemSecurity rogue package on offer has no utility other than scamming people out of their money. Variants of SystemSecurity have been around since at least February 2009. However, the Blue Screen of Death trick is a new social engineering innovation, only spotted in variants of the attack last week by anti-spyware firm Sunbelt Software. SystemSecurity usually makes its way onto compromised Windows PCs via fake video code installations. Users normally install the fake software (actually a Trojan horse) after following links in spam emails ostensibly inviting them to view video clips.



Password Length—It Does Matter (From frontlinedefenders.org)

Let's see how long it would take a computer program to guess your password. Assuming your password is made up only of lower-case English letters, we will calculate the maximum number of possibilities the password cracker needs to sort through.

Password Length	3	5	7	9
Calculation	26 x 26 x 26	26 x 26 x 26 x 26 x 26	26 x 26 x 26 x 26 x 26 x 26 x 26	26 x 26 x 26 x 26 x 26 x 26 x 26 x 26 x 26
Number of possibilities	17,576	11,881,376	8,031,810,176	54,295,503,678,976

Now, let's add digits and upper-case letters to our password. This increases the variations of every character to 62 different possibilities.

Password Length	3	5	7	9
Calculation	62 x 62 x 62	62 x 62 x 62 x 62 x 62	62 x 62 x 62 x 62 x 62 x 62 x 62	62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62
Number of possibilities	238,328	916,132,832	3,521,614,606,208	13,537,086,546,263,552

As you can see, the probabilities increase dramatically when you add variation into the password characters and when you increase its length. But how quickly can computers break these passwords? We will assume that a computer processes 100,000 password possibilities per second (modern PC). The table below shows password lengths from 3 to 12 characters. The figures at the top - 26, 36, 52, 68, 94 - indicate the number of characters from which the passwords are formed (assuming the English alphabet is used). 26 is the number of lower-case letters, 36 is letters and digits, 52 is mixed-case letters, 68 is single-case letters with digits, symbols and punctuation.

	26	36	52	68
3	0.18 seconds	0.47 seconds	1.41 seconds	3.14 seconds
4	4.57 seconds	16.8 seconds	1.22 minutes	3.56 minutes
5	1.98 minutes	10.1 minutes	1.06 hours	4.04 hours
6	51.5 minutes	6.05 hours	13.7 days	2.26 months
7	22.3 hours	9.07 days	3.91 months	2.13 years
8	24.2 days	10.7 months	17.0 years	1.45 centuries
9	1.72 years	32.2 years	8.82 centuries	9.86 millennia
10	44.8 years	1.16 millennia	45.8 millennia	670 millennia
11	11.6 centuries	41.7 millennia	2,384 millennia	45,582 millennia
12	30.3 millennia	1,503 millennia	123,946 millennia	3,099,562 millennia

Based on these figures, one can assume that even an 8-character random password using small-case letters and digits will be sufficient in complexity. If your main password to-date has been only 5 characters long, it is possible it has already been compromised, or is likely to be compromised, should the need arise.

Tables provided by Trainers in ITD

Password breakability comparing the length of the password to the number of possible characters.

Times are based on a modern computer processing 100,000 possibilities per second.

Seconds

Length	Single-case Letters	Single-case Letters & Numbers	Dual-case Letters	Single-case letters, numbers, symbols & punctuation
	26	36	52	68
3	0.18	0.47	1.41	3.14
4	4.57	16.80	73.12	213.81
5	118.81	604.66	3802.04	14539.34
6	3089.16	21767.82	197706.10	988674.83
7	80318.10	783641.64	10280717.03	67229888.18
8	2088270.65	28211099.07	534597285.31	4571632396.53
9	54295036.79	1015599566.68	27799058836.36	310871002964.30
10	1411670956.53	36561584400.63	1445551059490.57	21139228201572.10
11	36703444869.88	1316217038422.67	75168655093509.70	1437467517706900.00
12	954289566616.82	47383813383216.20	3908770064862500.00	97747791204069400.00

Hours

Length	Single-case Letters	Single-case Letters & Numbers	Dual-case Letters	Single-case letters, numbers, symbols & punctuation
	26	36	52	68
3	0.00	0.00	0.00	0.00
4	0.00	0.00	0.02	0.06
5	0.03	0.17	1.06	4.04
6	0.86	6.05	54.92	274.63
7	22.31	217.68	2855.75	18674.97
8	580.08	7836.42	148499.25	1269897.89
9	15081.95	282110.99	7721960.79	86353056.38
10	392130.82	10155995.67	401541960.97	5872007833.77
11	10195401.35	365615844.01	20880181970.42	399296532696.36
12	265080435.17	13162170384.23	1085769462461.81	27152164223352.60

Years

Length	Single-case Letters	Single-case Letters & Numbers	Dual-case Letters	Single-case letters, numbers, symbols & punctuation
	26	36	52	68
3	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.00
6	0.00	0.00	0.01	0.03
7	0.00	0.02	0.33	2.13
8	0.07	0.89	16.95	144.97
9	1.72	32.20	881.50	9857.65
10	44.76	1159.36	45838.12	670320.53
11	1163.86	41736.97	2383582.42	45581795.97
12	30260.32	1502530.87	123946285.67	3099562125.95

Millenia

Length	Single-case Letters	Single-case Letters & Numbers	Dual-case Letters	Single-case letters, numbers, symbols & punctuation
	26	36	52	68
3	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.00
6	0.00	0.00	0.00	0.00
7	0.00	0.00	0.00	0.00
8	0.00	0.00	0.02	0.14
9	0.00	0.03	0.88	9.86
10	0.04	1.16	45.84	670.32
11	1.16	41.74	2383.58	45581.80
12	30.26	1502.53	123946.29	3099562.13